New Jersey Chemical Sector
Checklist for Implementation of
Security Best Practices Standards

Company Name, DIFF #		
Local Name		
Person(s) Interviewed, Title		
Department Reviewer, Date		

This report was prepared at the direction of the New Jersey Domestic Security Preparedness Task Force pursuant to its authority under the New Jersey Domestic Security Preparedness Act. The information contained within this report is **CONFIDENTIAL** and shall be protected as privileged and confidential under the authorities of the New Jersey Domestic Security Preparedness Act, P.L. 2001, Ch. 246, N.J.S.A. App. A:9-69.6c and N.J.S.A. A:9-74.11.a, and the Toxic Catastrophe Prevention Act, N.J.S.A. 13:1K-29. This report shall not be deemed a public record under the provisions of P.L. 1963, c. 73 (C.47:1A-1 et seq.) or the common law concerning access to public records.

Security Requirement	**Yes**	**No**	**N/A**	**Comments**
Security Vulnerability Assessment (SVA)				
General				
1. Was an SVA conducted? List the date the SVA was completed or scheduled for completion.				
2. Was an approved SVA methodology used? Specify the methodology. (Air Products, API/NPRA, BASF, Bayer, CCPS, Easi-Assessment by Straec, ExxonMobil, FMC, Georgia Pacific, PPG, Sandia, SOCMA w/manual, SVA Pro by Dyadem,)				
3. Was a multi-disciplined team used to conduct the SVA?				
4. Was a "qualified security expert" part of the SVA team? If yes, list name, title, and affiliation.				

Security Requirement	**Yes**	**No**	**N/A**	**Comments**
5. Was a consultant used to prepare the SVA? If yes, list the name of the firm.				
6. Were employees afforded an opportunity to provide input? If yes, describe the mechanism employed.				
Facility Characterization				
1. Were the following critical assets identified?				
a. Equipment? List equipment that the facility identified as critical.				
b. Process control systems?				
c. Raw materials & products? List substances that the facility identified as critical.				
d. Utilities?				
e. Data?				
f. Personnel?				
2. Were on-site and off-site consequences of a successful attack documented and ranked as to the following?				
a. Impact to people?				
b. Impact to infrastructure?				
c. Impact to economy?				
d. Impact to environment?				
Threat Assessment				
1. Were the following potential adversaries identified, characterized, & ranked?				

Security Requirement	Yes	No	N/A	Comments
a. External? Describe the adversaries and rank (Only list the threats ranked medium & high).				
b. Internal? Describe the adversaries and rank (Only list the threats ranked medium & high).				
c. Internally assisted? Describe the adversaries and rank (Only list the threats ranked medium & high).				
2. Was the facility's target attractiveness analyzed? Summarize the facility's target attractiveness.				
Vulnerability Analysis				
1. Were specific threat scenarios defined?				
2. Did the scenarios address the following:				
a. Degradation of assets?				
b. Loss of containment?				
c. Theft?				
d. Contamination?				
e. IT system compromise?				
3. Were existing security systems evaluated and ranked based on:				
a. Ability to Deter?				
b. Ability to Detect?				
c. Ability to Delay?				

Security Requirement	Yes	No	N/A	Comments
d. Ability to Respond?				
4. Were vulnerabilities identified & ranked? Summarize the vulnerabilities and rank.				
Risk Reduction Recommendations				
1. Were risk reduction recommendations made?				
2. Were all recommendations implemented? If no, which were not, why, and when are they scheduled for completion.				
Prevention, Preparedness, and Response Plan				
Implementation of Best Practices				
1. Does the plan address communication with public & private groups?				
2. Does the plan address access control systems?				
3. Does the plan address perimeter protection?				
4. Does the plan address backup systems for utilities (for high-risk facilities only)?				
5. Does the plan address policies, procedures, and training for emergency response & security?				
6. Does the plan address transportation security procedures?				
7. Does the plan address cyber security?				